Configuración del concentrador Cisco VPN 3000 en un router Cisco

Contenido

Introducción

Esta configuración de muestra muestra cómo conectar una red privada detrás de un router que funcione con el software del ® del Cisco IOS a una red privada detrás del Cisco VPN 3000 Concentrator. Los dispositivos de las redes se reconocen entre sí por las direcciones privadas.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 2611 Router con la versión de Cisco IOS Software 12.3.(1)a**Note**: Aseegurese que los

Cisco 2600 Series Router están instalados con una imagen del IOS crypto del IPSec VPN que soporte la característica VPN.
- Cisco VPN 3000 Concentrator con 4.0.1 B

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

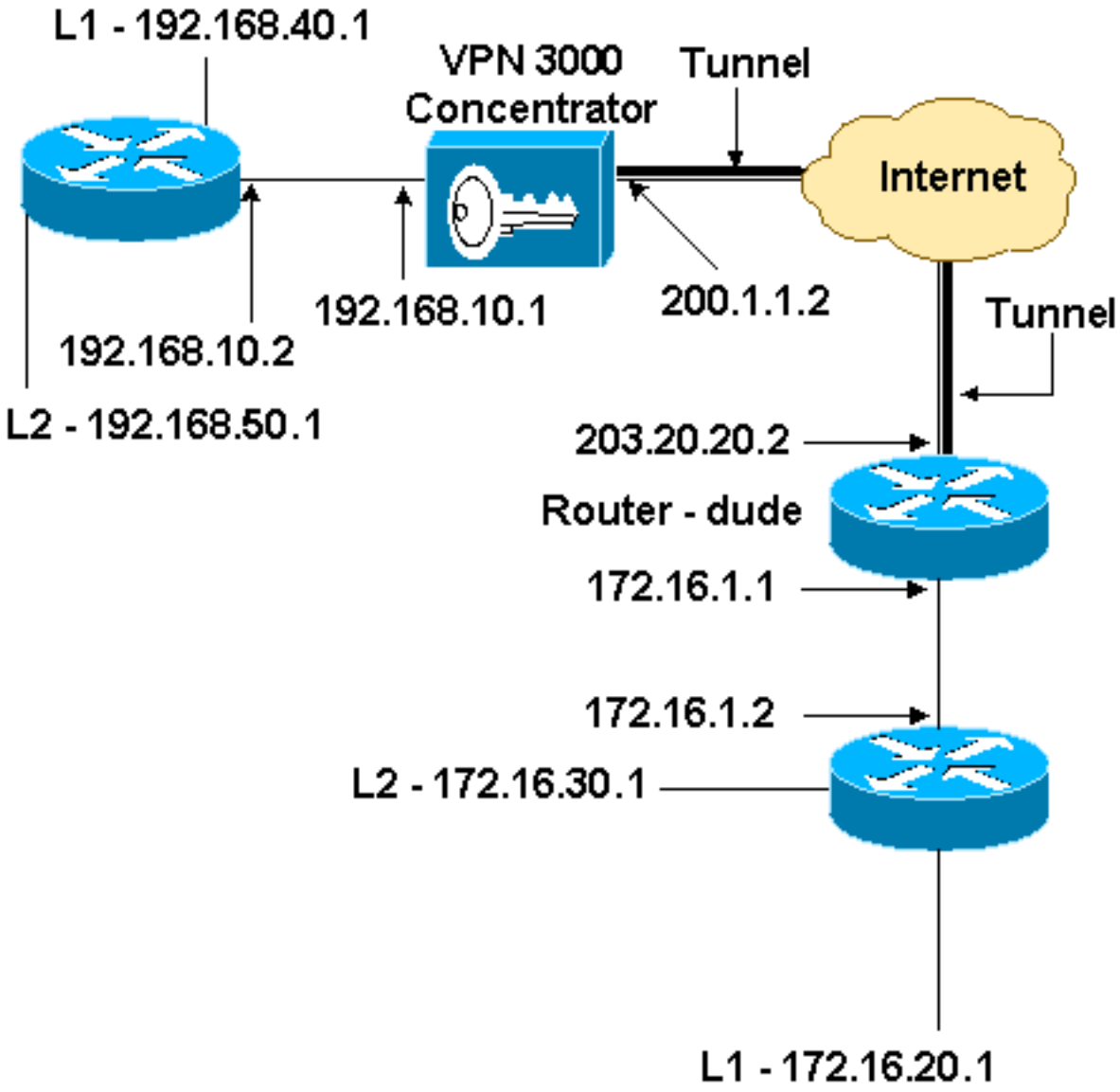
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Note: Use la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados en este documento.

Diagrama de la red

Este documento utiliza esta configuración de red:



Configuraciones

Este documento utiliza esta configuración.

Configuración del router

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 200.1.1.2
```

```
!!--- IPsec policies. crypto ipsec transform-set to_vpn
esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set to_vpn
!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
 ip address 203.20.20.2 255.255.255.0
 ip nat outside
 half-duplex
 crypto map to_vpn
!
interface Ethernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip
172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
!--- Traffic to except from the NAT process. access-list
110 deny   ip 172.16.1.0 0.0.0.255 192.168.10.0
0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
```

```
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end
```

Configuración del concentrador VPN

En este entorno de laboratorio, el concentrador VPN primero se accede a través del puerto de la consola y se agrega una configuración mínima para poder hacer la configuración posterior con el Interfaz gráfica del usuario (GUI).

Elija el **Administration (Administración)> System reboot (Reinicio del sistema) > Schedule Reboot (Reinicio del programa) > Reboot with Factory/Default Configuration (Reinicio con configuración predeterminada/de fábrica)** para asegurarse de que no hay configuración existente en el concentrador VPN.

El concentrador VPN aparece en configuración rápida, y estos elementos se configuran después de la reinicialización:

- Fecha/hora
- Interfaces/Masks in Configuration > Interfaces (public=200.1.1.2/24, private=192.168.10.1/24)
- Gateway predeterminada en Configuration (Configuración) > System (Sistema) > ip routing (Ruteo de IP) > Default_Gateway (200.1.1.1) (Gateway predeterminada [200.1.1.1])

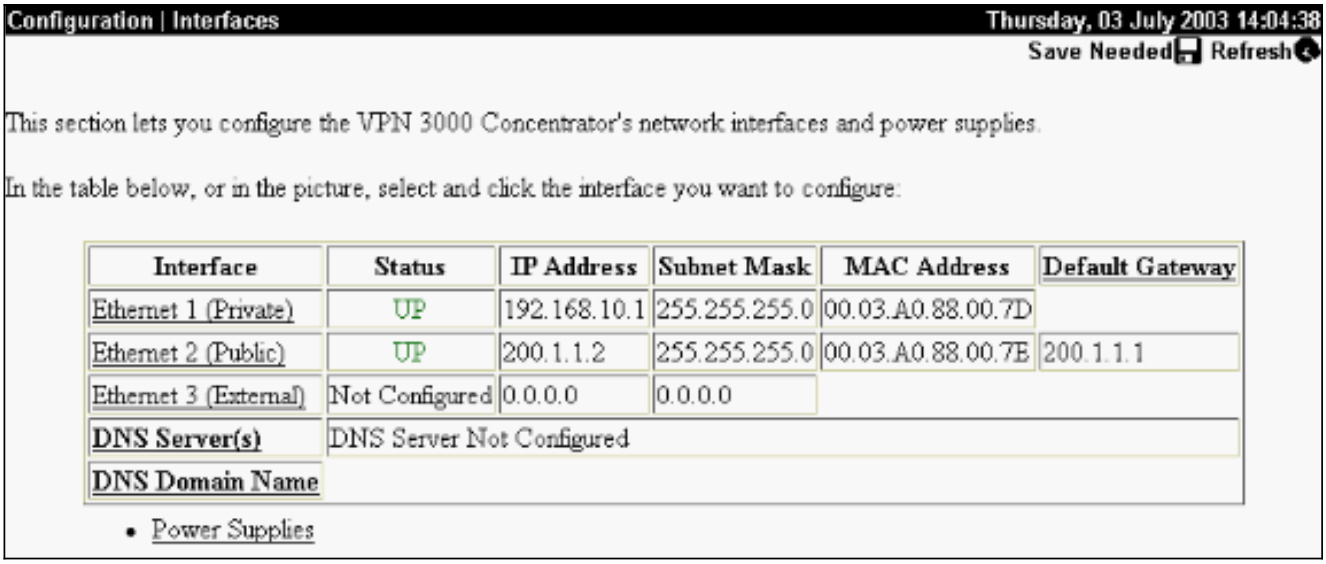
En este momento, el concentrador VPN es accesible con el HTML de la red interna.

Note: Porque el concentrador VPN se maneja de afuera, usted también tiene que seleccionar:

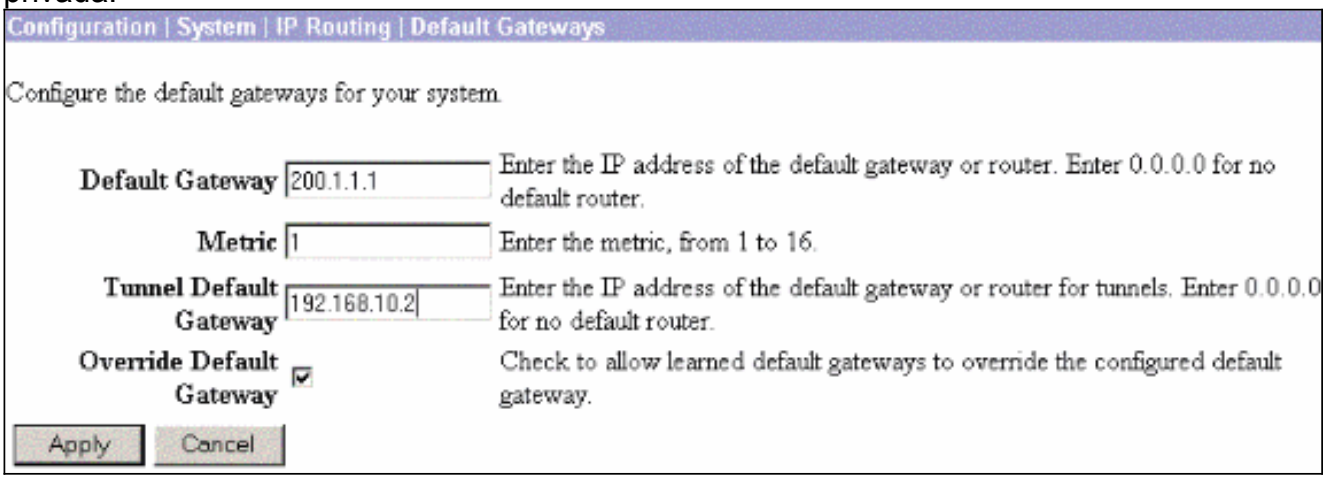
- **Configuration (Configuración) > Interfaces (Interfaces) > 2-public > filtro IP selecto > 1. soldados (valor por defecto)**.
- **Administration (Administración) > Access Rights (Derechos de acceso) > Access Control List (Lista de control de acceso)** > Add Manager Workstation para agregar la dirección IP del *administrador externo*.

Esto no es necesario a menos que usted maneje el concentrador VPN del *exterior*.

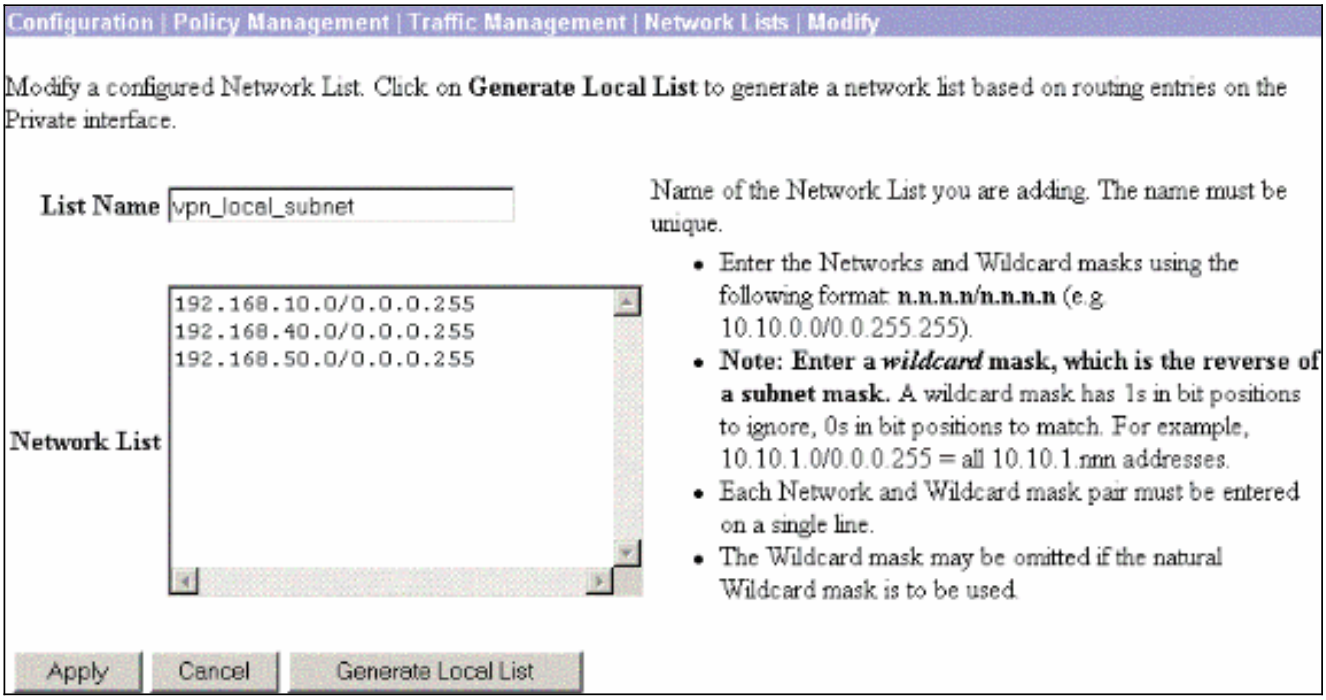
1. Elija el **Configuration (Configuración) > Interfaces (Interfaces)** para volver a inspeccionar las interfaces después de que usted traiga para arriba el GUI.



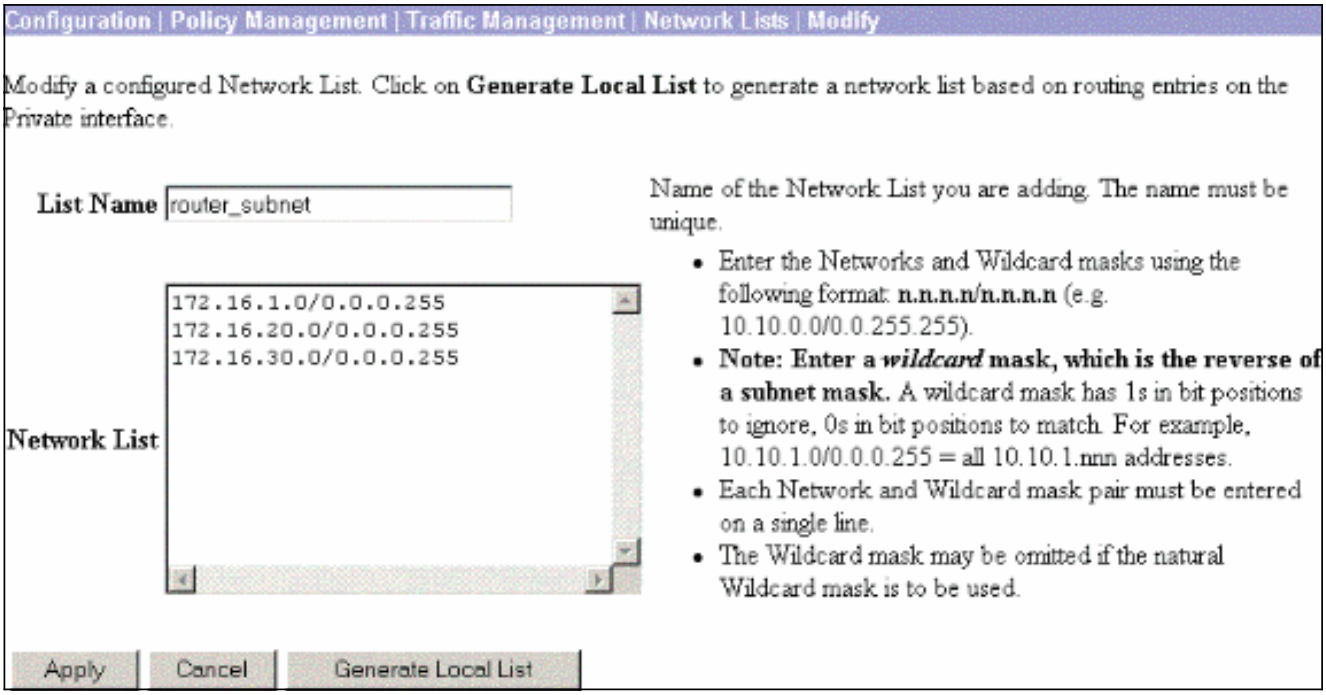
2. Elija **Configuration > System > Routing IP >** los **default gatewayes** para configurar el **gateway predeterminado** (de Internet) y el **gateway del valor por defecto del túnel** (dentro) para que el IPSec alcance las otras subredes en la red privada.



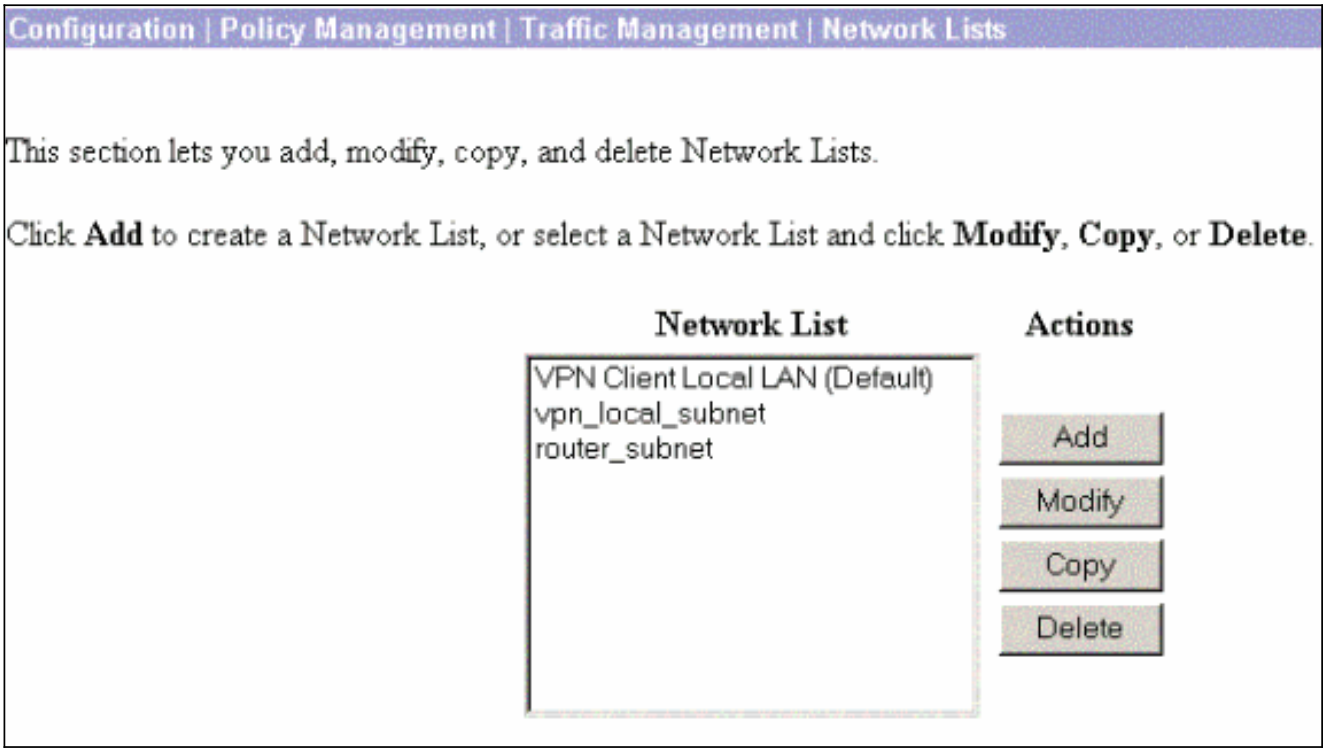
3. Elija **Configuration > Policy Management >** Network Lists crear las listas de red que definen el tráfico que se cifrará.Éstas son las redes locales:



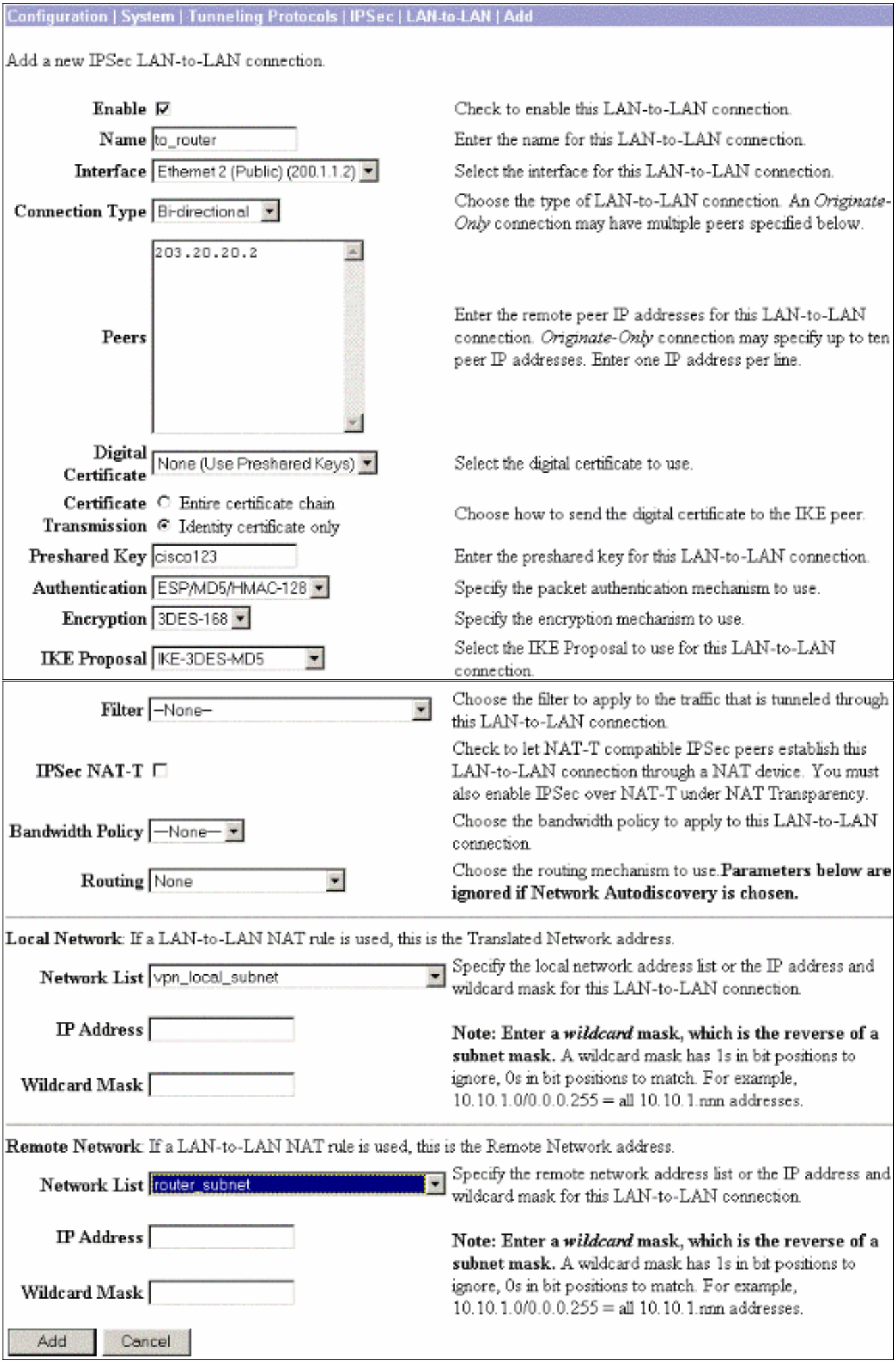
Éstas son las redes
remotas:



4. Una vez terminado, estas son las dos listas de red:**Note**: Si no sube el túnel IPsec, marcar para ver si el tráfico interesante hace juego en los ambos lados. El tráfico interesante es definido por la lista de acceso en el router y los cuadros PIX. Son definidos por las listas de red en los concentradores
VPN.

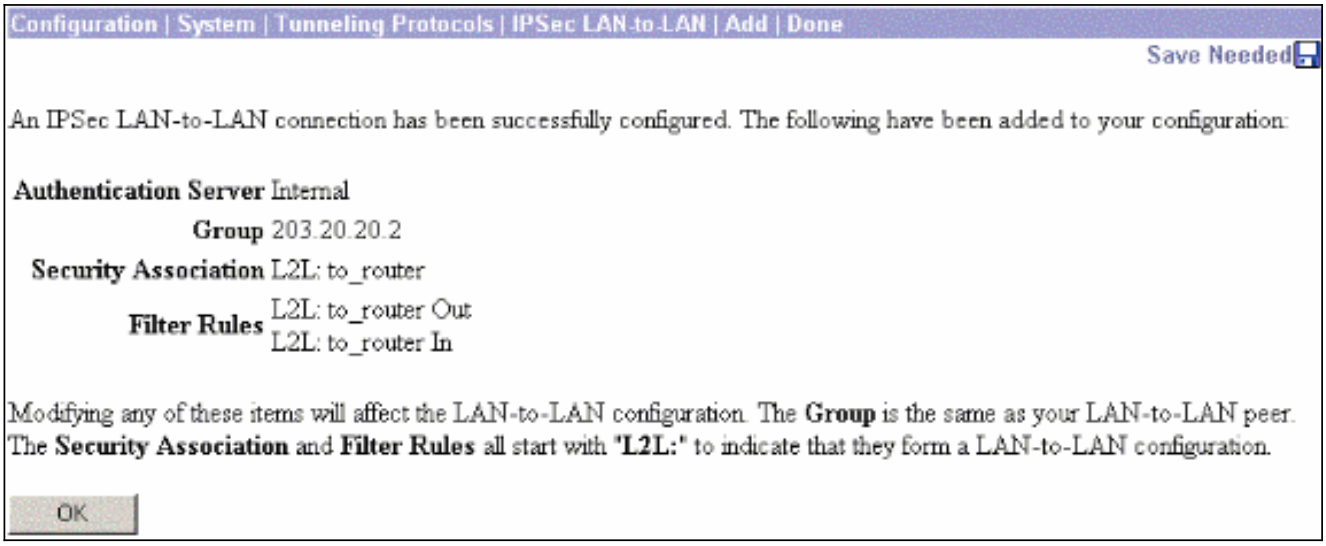


5. Elija el **Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec LAN-to-LAN (IPSec de LAN a LAN)** y defina el túnel de LAN a LAN.

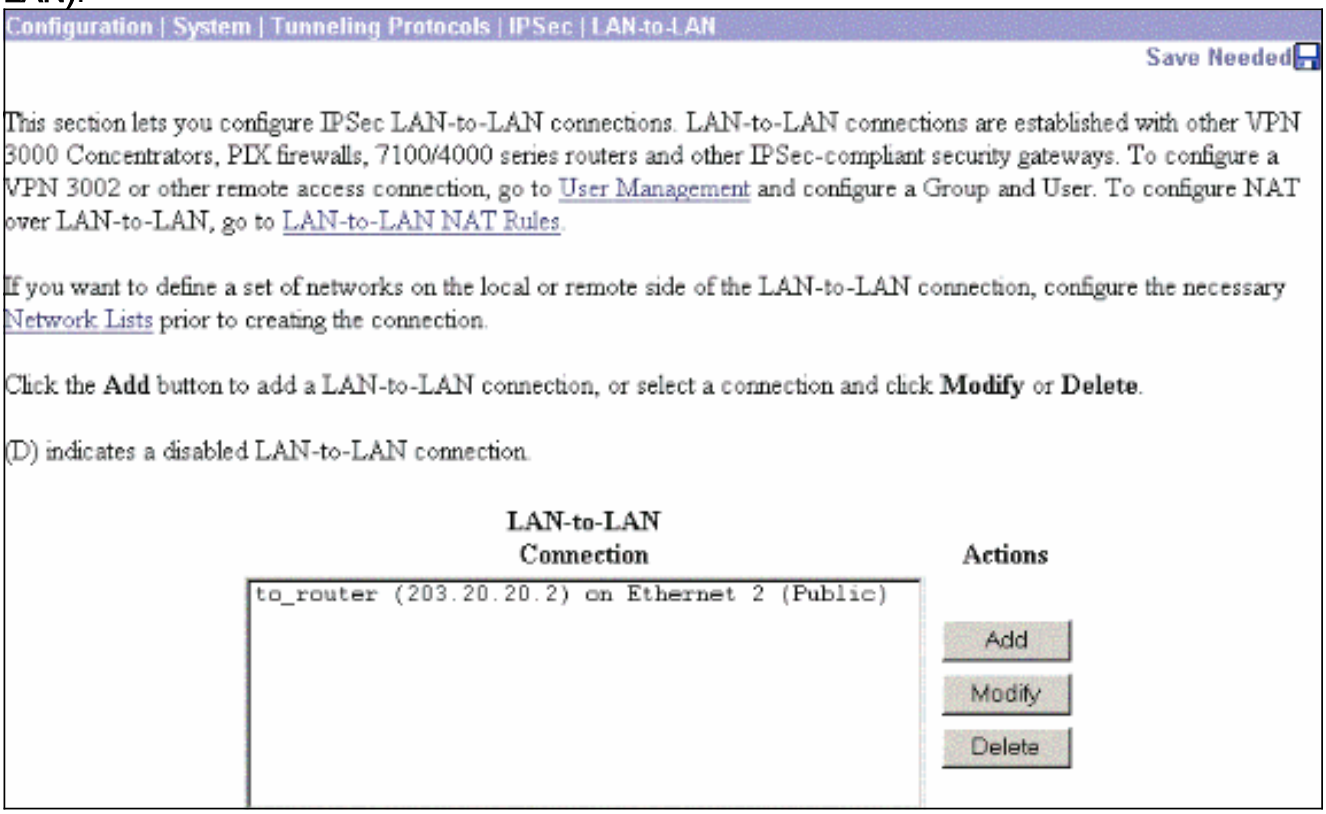


6. Después de que usted tecleo **se aplique**, esta ventana se visualiza con la otra configuración

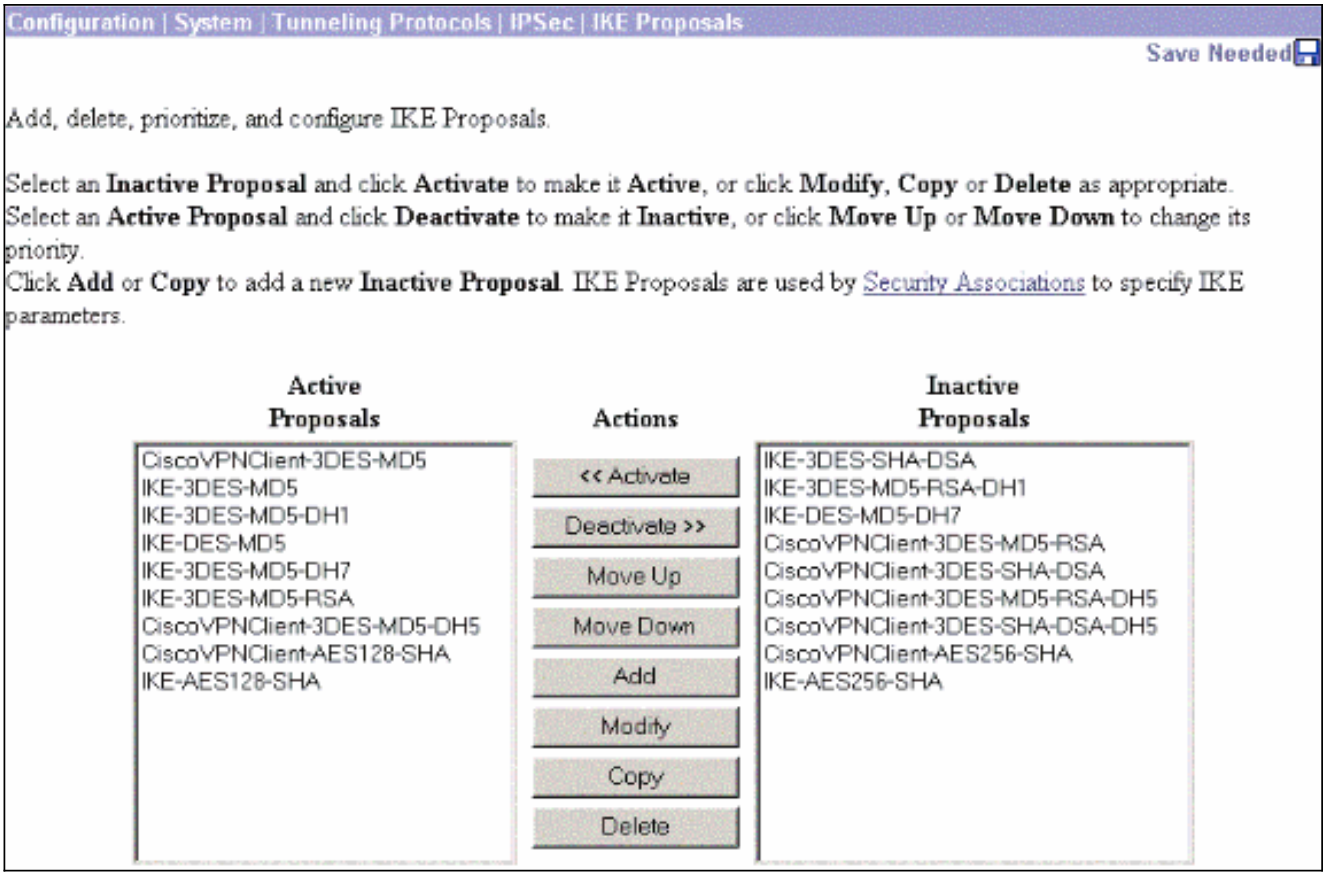
que se crea automáticamente como resultado del configuración del túnel de LAN a LAN.



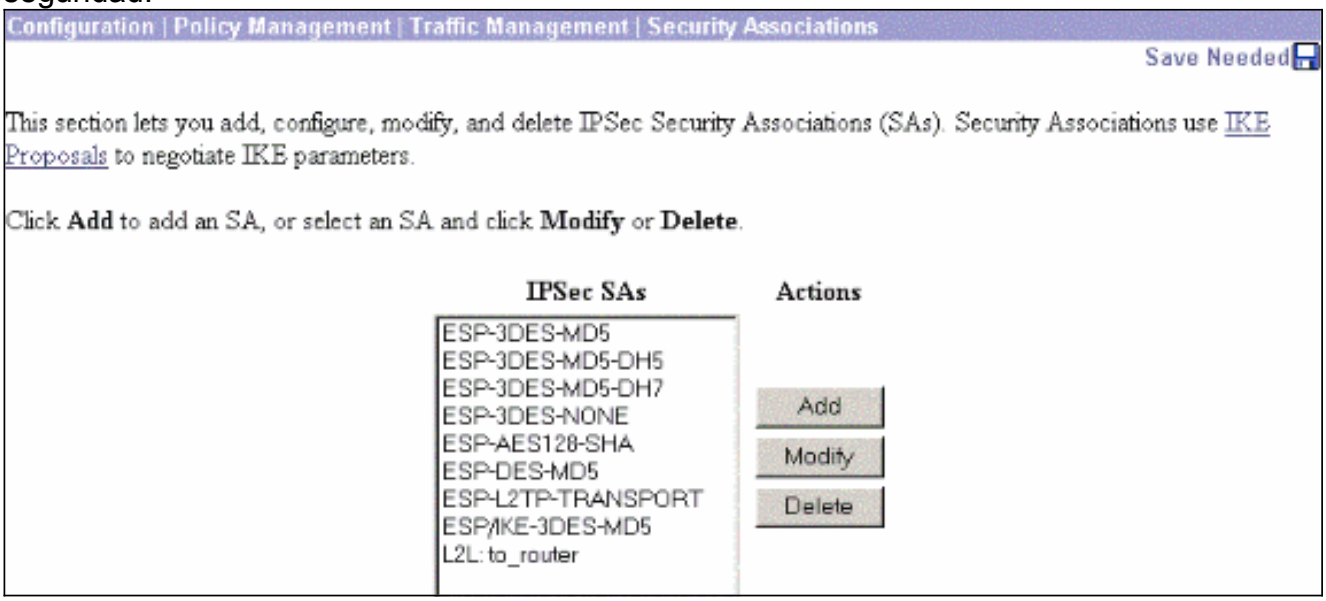
Los parámetros de IPSec previamente creados del LAN a LAN se pueden ver o modificar en el **Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec LAN-to-LAN (IPSec de LAN a LAN)**.



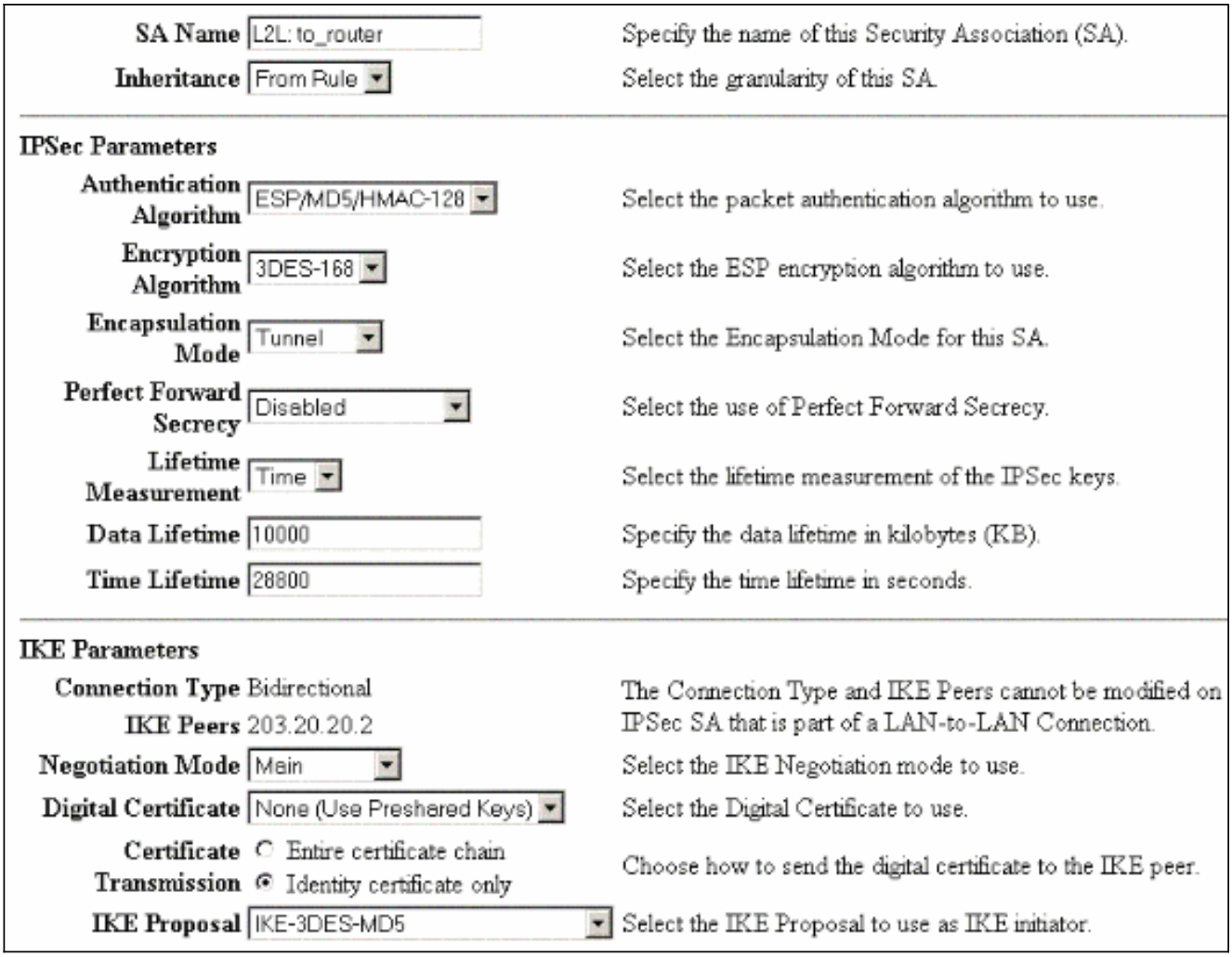
7. Elija el **Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec > IKE Proposals (Propuestas IKE)** para confirmar la oferta del IKE activo.



8. Elija el **Configuration (Configuración) > Policy Management (Administración de políticas) > Management Traffic (Administración de tráfico) > Security Associations (Asociaciones de seguridad)** para ver la lista de asociaciones de seguridad.



9. Haga clic el Security Association name, y después haga clic **se modifican** para verificar las asociaciones de seguridad.



Verificación

Esta sección enumera los **comandos show** usados en esta configuración.

En el router

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- show crypto ipsec sa - Muestra las configuraciones usadas por las asociaciones de seguridad actuales.
- **muestre isakmp crypto sa** — Muestra todas las asociaciones actuales de la seguridad de intercambio dominante de Internet en un par.
- **show crypto engine connection active** — Muestra las conexiones de sesión encriptada activas actuales para todos los motores de criptografía.

Usted puede utilizar la herramienta de búsqueda de comandos del IOS (clientes registrados solamente) para ver más información sobre los comandos determinados.

En el concentrador VPN

Elija el **Configuration (Configuración) > System (Sistema) > Events (Eventos) > Classes (Clases) > Modify (Modificar)** para dar vuelta encendido a la registración. Estas opciones están disponibles:

- IKE
- IKEDBG
- IKEDECODE
- IPSEC
- IPSECDBG
- IPSECDECODE

Gravedad de registro = 1-13

Gravedad en la consola = 1-3

Seleccione el **Monitoring (Monitoreo) > Event Log (Registro de evento)** para extraer el registro de acontecimientos.

Troubleshooting

En el router

Refiera a la información importante en los comandos Debug antes de que usted intente cualquier comando debug.

- debug crypto engine - Muestra el tráfico cifrado.
- **IPSec del debug crypto** — Visualiza los IPSec Negotiations de la fase 2.
- **isakmp del debug crypto** — Visualiza negociaciones ISAKMP de la fase 1.

Problema - Incapaz de iniciar el túnel

Mensaje de error

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 200.1.1.2
!!--- IPsec policies. crypto ipsec transform-set to_vpn esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
 set peer 200.1.1.2
```

```
 set transform-set to_vpn
!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
 ip address 203.20.20.2 255.255.255.0
 ip nat outside
 half-duplex
 crypto map to_vpn
!
interface Ethernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask 255.255.255.0
ip nat inside source route-map nonat pool mypool overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.50.0 0.0.0.255
!--- Traffic to except from the NAT process. access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end
```

Solución

Complete esta acción para configurar el número deseado de logines simultáneos o fijar los logines simultáneos a 5 para este SA:

Van al **Configuration (Configuración)>User Management (Administración del usuario) >Groups (Grupos) > Modify 10.19.187.229 > los logines del general > de Simultaneouts** y cambian el número de logines a 5.

PFS

En las negociaciones de IPSec, Perfect Forward Secrecy (PFS) garantiza que cada clave criptográfica nueva no esté relacionada a cualquier clave anterior. Habilite o inhabilite el PFS en ambos los peeres de túnel. Si no, el túnel IPsec del LAN a LAN (L2L) no se establece en el Routers.

Para especificar que el IPSec debe pedir el PFS cuando solicitan las nuevas asociaciones de seguridad para esta entrada de correspondencia de criptografía, o que el IPSec requiere el PFS cuando recibe los pedidos las nuevas asociaciones de seguridad, utiliza el **comando set pfs** en el modo de configuración de la correspondencia de criptografía. Para especificar que el IPSec no debe pedir el PFS, no utilice la **ninguna** forma de este comando.

```
set pfs [group1 | group2]
no set pfs
```

Para el comando set pfs:

- *group1* — Especifica que el IPSec debe utilizar el grupo del módulo de la prima de Diffie Hellman del 768-bit cuando el nuevo intercambio Diffie-Hellman se realiza.
- *group2* — Especifica que el IPSec debe utilizar el grupo del módulo de la prima 1024-bit Diffie Hellman cuando el nuevo intercambio Diffie-Hellman se realiza.

De forma predeterminada, PFS no se solicita. Si no se especifica ningún grupo con este comando, como valor predeterminado se utiliza group1.

Ejemplo:

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

Refiera a la referencia de comandos de la Seguridad de Cisco IOS para más información sobre el **comando set pfs**.

Información Relacionada

- Soluciones a los Problemas más frecuentes de IPSec VPN L2L y de Acceso Remoto
- Cisco VPN 3000 Series Concentrators
- Cisco VPN 3002 Hardware Clients
- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems